Claims

1. Method for producing a payload data stream comprising a header and a payload data block containing encrypted payload data, comprising the following steps:

generating a payload data key for a payload data encryption algorithm for encrypting payload data;

encrypting payload data using said payload data key and said payload data encryption algorithm to obtain an encrypted section of said payload data block of said payload data stream;

processing a part of said payload data stream to deduce information marking said part of said payload data stream;

linking said information containing said payload data key by means of an invertible logic linkage to obtain a basic value;

encrypting said basic value using a key of two keys being different from each other by an asymmetrical encryption method, said two different keys being the public and the private keys respectively for said asymmetrical encryption method, to obtain an output value being an encrypted version of said payload data key; and

entering said output value into said header of said payload data stream.

2. Method according to claim 1, in which said payload data encryption algorithm is a symmetrical encryption algorithm.

3. Method according to claim 1, in which said invertible logic linkage is self-inverting and includes an XOR-linkage.

4. Method according to claim 1, in which one key of said two keys being different from each other is the private key of a producer of said payload data stream or the public key of a consumer of said payload data stream.

5. Method according to claim 1, in which said part of said payload data stream being processed to deduce said information includes at least a part of said header.

6. Method according to claim 1, in which said step of processing comprises forming a hash sum.

7. Method according to claim 1, further comprising the following step:

identifying said algorithm being used in said step of processing by an entry into said header.

8. Method according to claim 1, further comprising the following step:

entering license data into said header, said data referring to in which way said payload data stream is allowed to be employed.

9. Method according to claim 8, in which said license data indicates how often said payload data stream is allowed to be replayed and how often it has already been replayed.

10. Method according to claim 8, in which said license data indicates how often the contents of said payload data stream is allowed to be copied and how often it has already been copied.

11. Method according to claim 1, in which said license data indicates from when on said payload data stream is no longer allowed to be employed.

12. Method according to claim 8, in which said license data indicates from when on said payload data stream is allowed to be decrypted.

13. Method according to claim 8, in which said part of said payload data stream being processed to deduce said information includes said license data.

14. Method according to claim 1, in which said step of processing further comprises the following substep:

setting said entry for said output value in said header to a defined value and processing said entire header, including said entry set to a defined value.

15. Method according to claim 1, further comprising the following steps:

identifying the supplier of said payload data stream by a supplier entry into said header;

identifying the user of said payload data stream by a user entry into said header of said payload data stream,

said supplier entry and said user entry belonging to said part of said payload data stream being processed to deduce said information.

16. Method according to claim 1, further comprising the following step:

identifying said payload data encryption algorithm by an entry into said header of said payload data stream.

17. Method for decrypting an encrypted payload data stream comprising a header and a payload data block containing encrypted payload data, said header comprising an output value having been generated by an encryption of a basic value by an asymmetrical encryption method using a key of two different keys including a private and a public key, said basic value representing a linkage of a payload data key, with which said encrypted payload data is encrypted using a payload data encryption algorithm, and information deduced by a certain processing, said information marking a certain part of said payload data stream

unambiguously, said method comprising the following steps:

obtaining said output value from said header;

decrypting said output value using the other key of said asymmetrical encryption method to obtain said basic value;

processing a part of said payload data stream using the processing method used for encrypting to deduce information marking said part, said part corresponding to said certain part when encrypting;

linking said information and said basic value using the corresponding linkage as it has been used when encrypting to obtain said payload data key; and

decrypting said block containing encrypted payload data using said payload data key and said payload data encryption algorithm used when encrypting.

18. Method according to claim 17, in which said header comprises license information referring to in what way said payload data stream can be employed.

19. Method according to claim 17, in which said part being processed to deduce said information is said header.

20. Method according to claim 18, further comprising the following steps:

checking whether said license information allows a decryption; and

if a decryption is not allowed, cancelling said decryption method.

21. Method according to claim 17, in which said header comprises a user entry, said method further comprising the following steps:

checking by means of said user entry whether a current user is authorized; and

if the user is not authorized, cancelling said decryption method.

22. Method according to claim 17, in which one key having been used when encrypting is the private key of said asymmetrical encryption method, while the other key having been used when decrypting is the public key of said asymmetrical encryption method.

23. Method according to claim 17, in which one key having been used when encrypting is the public key of said asymmetrical encryption method, while the other key having been used when decrypting is the private key of said asymmetrical encryption method.

24. Method according to claim 17, in which said step of processing includes forming a hash sum.

25. Method according to claim 17, in which a part of said header having been set to a defined value for said

step of processing when encrypting is set to the same defined value for said step of processing when decrypting.

26. Method according to claim 25, in which said part of said header being set to a defined value includes said entry for said output value of said header.

27. Method according to claim 17, in which said step of linking comprises using an XOR-linkage.

28. Device for producing an encrypted payload data stream comprising a header and a payload data block containing encrypted payload data, comprising:

means for generating a payload data key for a payload data encryption algorithm for encrypting said payload data;

means for encrypting payload data using said payload data key and said payload data encryption algorithm to obtain an encrypted section of said payload data block of said payload data stream;

means for processing a part of said payload data stream to deduce information marking said part of said payload data stream;

means for linking said information and said payload data key by means of an invertible logic linkage to obtain a basic value;

means for encrypting said basic value using a key of two keys being different from each other by an asymmetrical encryption method, said two different keys being the public and the private keys respectively for said asymmetrical encryption method to obtain an output value being an encrypted version of said payload data key; and

means for entering said output value into said header of said payload data stream.

29. Device according to claim 28, which is implemented as a personal computer, a stereo system, a car hi-fi instrument, a solid state player or a replay instrument containing a hard disk or a CD-ROM.

30. Device for decrypting an encrypted payload data stream comprising a header and a block containing encrypted payload data, said header comprising an output value having been generated by an encryption of a basic value by an asymmetrical encryption method using a key of two different keys including a private and a public key, said basic value representing a linkage of a payload data key, with which said encrypted payload data is encrypted using a payload data encryption algorithm, and information deduced by a certain processing, said information marking a certain part of said payload data stream unambiguously, said device further comprising:

means for obtaining said output value from said header;

means for decrypting said output value using said other key and said asymmetrical encryption method to obtain said basic value;

means for processing a part of said payload data stream using the processing method used when encrypting to deduce information marking said part, said part corresponding to said certain part when encrypting;

means for linking said information and said basic value using the corresponding linkage as it has been used when encrypting to obtain said payload data key; and

means for decrypting said block containing encrypted payload data using said payload data key and said payload data encryption algorithm used when encrypting.

31. Device according to claim 30, which is implemented as a personal computer, a stereo system, a car hi-fi instrument, a solid state player or a replay instrument containing a hard disk or a CD-ROM.